BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenl gungsschrift**

(10) **DE 197 10 249 A 1**

(51) Int. Cl.[6]:
G 07 F 19/00
G 07 F 7/08
H 04 L 9/00

(21) Aktenzeichen: 197 10 249.2
(22) Anmeldetag: 12. 3. 97
(43) Offenlegungstag: 17. 9. 98

(71) Anmelder:
Siemens Nixdorf Informationssysteme AG, 33106 Paderborn, DE

(74) Vertreter:
Epping, W., Dipl.-Ing. Dr.-Ing., Pat.-Anw., 82131 Gauting

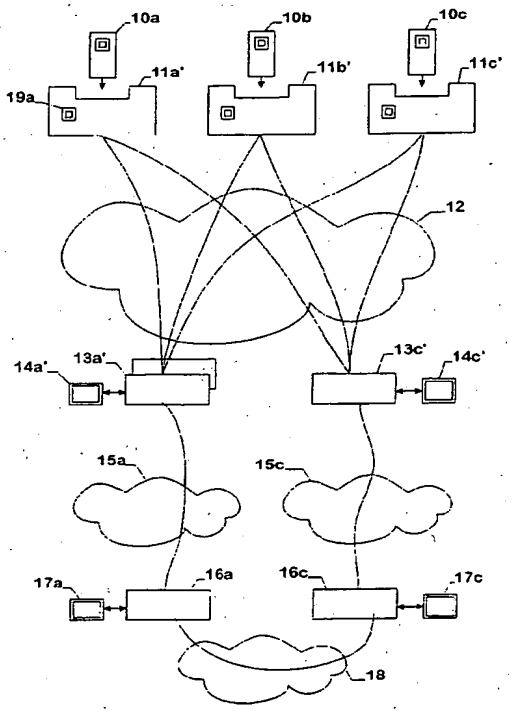
(72) Erfinder:
Wiehler, Gerhard, 82223 Eichenau, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Netzwerkunterstütztes Chipkarten-Transaktionsverfahren

(57) Terminals für die Abrechnung von Zahlungen sind über ein offenes Datennetzwerk mit gegen Manipulationen gesichertem Übertragungsverfahren mit einer Vielzahl von Abwicklern verbindbar, wobei aus der Art der Transaktion der Abwickler bestimmt wird.



DE 197 10 249 A 1

DE 197 10 249 A 1

Beschreibung

Technisches Gebiet

Die Erfindung betrifft Verfahren und Anordnungen für die elektronische Abrechnung von Leistungen, insbesondere durch Zahlungen, mittels Chipkarten unter Verwendung von offenen Datennetzwerken.

Stand der Technik

Zur Bezahlung von Leistungen werden Karten mit eingebettetem Prozessor oder Speicher, als Chipkarten bekannt, eingesetzt. Hierbei sind eine Anzahl verschiedener Kartenarten bekannt, die als "Creditcard", "Debitcard", vorausbezahlte Geldkarte oder als Geldkarte mit einer aufladbaren elektronischen Börse bekannt sind.

In vielen Ländern gibt es heute Geldkarten-Lösungen, die jeweils national entwickelt und spezifiziert sind; z. B. "Avant" in Finnland, "Danmønt" in Dänemark, die EC-Karte mit Chip in Deutschland, "Quick" in Österreich. Diese Lösungen sind in Technik und Verfahren untereinander inkompatibel.

Die Kreditkartenorganisationen testen derzeit Lösungen, die international zum Einsatz kommen sollen, z. B. "Visacash" von Visa, "Mondex" von Mastercard, "Clip" von Europay, "Proton" von American Express. Diese Lösungen sind gleichfalls untereinander inkompatibel. Obwohl diese Gruppe von Anbietern einen gemeinsamen Standard, der derzeit unter dem Arbeitstitel "EMV" bekannt ist, spezifiziert hat, so werden hierbei bereits ausgegebene Karten und im Markt befindliche Lösungen nicht berücksichtigt.

Es hat sich gezeigt, daß ein Teil dieser Karten zwar durchaus größtenteils dieselben Hardware-Einrichtungen nutzen, aber durch unterschiedliche Software-Programme und -Protokolle und spezifische Sicherheitsmodule in dem die Chipkarte aufnehmenden Terminal unterschieden sind. Demgemäß wurden Lösungen bekannt, bei denen ein Chipkarten-Terminal, das die Chipkarte während eines Bezahlvorgangs bedient, mit einer Anzahl von verschiedenen Software-Moduln ausgestattet ist und an das mehrere Sicherheitsmodule angeschlossen sind. Diese Lösung ist jedoch, weil teuer und unflexibel, nicht für den flächendeckenden Einsatz geeignet.

Aufgabe der Erfindung ist es daher, eine Lösung anzugeben, bei der flächendeckend eine große Anzahl verschiedener Chipkarten anwendbar ist, ohne daß jedes Terminal für alle dieser Chipkarten ausgerüstet sein muß.

Darstellung der Erfindung

Die Erfindung verwendet Chipkarten-Terminals, die an ein offenes Datenübertragungsnetzwerk angeschlossen sind, über das sie mit verschiedenen Abwicklern eine manipulationsgeschützte Verbindung aufbauen können, wobei aus der Art der Transaktion, bestimmt durch die Chipkarte, der Abwickler bestimmt wird.

Kurzbeschreibung der Zeichnungen

Es zeigen

Fig. 1 eine schematische Übersicht über die Komponenten bei einer Transaktionsabwicklung mit einer Chipkarte gemäß der Erfindung,

Fig. 2 eine **Fig.** 1 entsprechende Darstellung des Standes der Technik.

Beschreibung der Erfindung

In **Fig.** 2 ist eine bekannte Anordnung zur Transaktionsabwicklung von Zahlungen mit Chipkarten dargestellt. Im folgenden stehen dabei Zahlungen stellvertretend für alle Arten von Transaktionen, bei denen Wert auf zuverlässige Abwicklung gelegt wird. Als Chipkarten werden beispielsweise solche nach ISO 7816-1, -2, -3 eingesetzt.

Dabei sind Chipkarten **10a**, **10b** und **10c** mit Terminals **11a**, **11b**, **11c** verbindbar. Jedes Terminal enthält einen Abwickler **13a**, **13b1**, **13b2**, **13c**, der mit jeweils einem Sicherheitsmodul **14a**, **14b1**, **14b2**, **14c** verbunden ist. Die gezeigte Konfiguration bezieht sich auf zwei Zahlungsnetzwerke **15a**, **15c**, in denen ein Host **16a**, **16c** seinerseits jeweils einen Sicherheitsmodul **17a**, **17c** enthält und die Hosts über ein weiteres Netzwerk **18** untereinander Transaktionsdaten austauschen können. Anstelle von Sicherheitsmoduln können auch die Hosts in gesicherter Umgebung mit beispielsweise strenger Zugangskontrolle betrieben werden und die Schlüssel auf üblichen Datenträgern ablegt sein. Die Netzwerke **15a**, **15c** sind beispielsweise X25/Datex-P-Netzwerke, meist als geschlossene Benutzergruppen geschaltet. Das Terminal **11a** ist dem Host **16a**, das Terminal **11c** dem Host **16c** zugeordnet und kann daher nur solche Verfahren abwickeln, die von dem Host unterstützt werden. In der Regel ist der jeweilige Abwickler **13a**, **13c** für den Anbieter bzw. den Dienst, im folgenden auch Transaktionsart, spezifisch. Hierbei stehen auch im folgenden Hosts auch stellvertretend für hierarchische oder vermaschte Netzwerke von Rechnern, für die der Host den Zugang und die Schnittstelle darstellt.

Um daher in dem Terminal **11b** zwei verschiedene Karten für die beiden verschiedenen Dienste benutzbar zu machen, sind in dem Terminal **11b** zwei Abwickler **13b1**, **13b2** vorgesehen, die jeweils mit einem eigenen Sicherheitsmodul **14b1**, **14b2** verbunden sind und jeweils einen eigenen, dedizierten Netzwerkanschluß an das jeweilige Netzwerk **15a**, **15c** besitzen.

Solange nur wenige Terminals und wenige Dienste vorhanden sind, ist der Aufwand der mehrfachen Abwickler in einem Terminal möglich.

Die Erfindung nun trennt den Abwickler von dem Terminal und ist wie in **Fig.** 1 dargestellt angeordnet. Hierbei enthalten die Terminals **11a'**, **11b'**, **11c'** keinen Abwickler bisheriger Art mehr. Es ist lediglich ein Betriebsprogramm, welches nicht gesondert dargestellt ist, vorhanden, das die Kommunikation zur Chipkarte **10a**, **10b**, **10c** bewirkt und für eine gesicherte Verbindung zu verschiedenen Abwicklern **13a'**, **13c'** dient.

Ein offenes Netzwerk **12** übernimmt die Datenvermittlung zwischen den Terminals **11a'**, **11b'**, **11c'** und Abwicklern **13a'**, **13c'**, welche wiederum wie in herkömmlicher Weise über spezifische Netzwerke **15a**, **15c** mit den Hosts **16a**, **16c** zusammenwirken. Über diese Netzwerke können weiterhin und zusätzlich Chipkarten-Terminals bekannter Art betrieben werden.

Dieses Netzwerk **12** ist vorzugsweise ein offenes Netzwerk, wie es durch das Internet und die IP-Protokollfamilie im folgenden repräsentiert ist. Durch die allgemeine Verfügbarkeit und offene Architektur ist es jedem der Terminals **11a'**, **11b'** und **11c'** ohne weiteres möglich, jeden der Abwickler **13a'**, **13c'** zu erreichen. Jedes Terminal kann nun, wie noch genauer beschrieben wird, jeden Abwickler erreichen und damit jede Chipkarte annehmen und Transaktionen abwickeln, sofern auch nur ein passender Abwickler im Netz erreichbar ist. Auch ist es sinnvoll, mehrere Abwickler an einem Ort bereitzustellen, wie in **Fig.** 1 für den Abwickler **13a'** dargestellt ist, weil eine Vielzahl von Terminals dar-

auf zugreifen kann und die einmalige Installation nur eines einzigen Abwicklers unmittelbar allen Terminals zur Verfügung steht.

Dabei muß das Betriebsprogramm in dem Terminal zunächst die Art der Chipkarte ermitteln, d. h., den Dienst bzw. das anzuwendenden Transaktionsprotokoll und damit einen möglichen Abwickler ermitteln. Dies geschieht durch Auslesen aus der Chipkarte. Chipkarten können auch mehrere Dienste unterstützen; in diesem Fall müßte das Terminal den Benutzer fragen, mit welchem Dienst bezahlt werden soll, sofern dies nicht implizit entschieden werden kann. Bei einer Kreditkarte mit aufladbarer elektronischer Geldbörse könnten beispielsweise Beträge unter DM 20 immer von der Geldbörse und hohe Beträge von der Kreditkartenfunktion abgebucht werden.

Aus dem gewünschten Dienst wird dann beispielsweise ein "uniform resource locator", (URL), gebildet. Dies kann durch eine Tabelle im Terminal oder durch Anfrage bei einem Abwickler ermittelt werden. Die Verwendung einer URL ist insofern vorteilhaft, weil sie eine Tabelle im Terminal entbehrlich macht, weil die Netzwerkfunktionen dann den nächstliegenden Abwickler für diesen Dienst ermitteln. Ein URL für eine Gold-Kreditkarte von American Express könnte dann lauten

"https://de.amexco.com/credit/gold/Hamburg"

wobei "https" das Protokoll für die Datenübermittlung zwischen Terminal und Abwickler kennzeichnet. In dem URL sind, wie in dem Beispiel ersichtlich, sowohl der Standort in dem Rechnernamen "de.amexco.com" als auch die Stadt codierbar. Durch die Codierung des Rechnernamens wird zwar die Internetadresse gegebenenfalls über den authorisierten Namensserver der Zentrale in den USA angefordert, aber dieser kann auf einen Rechner in Deutschland weisen, so daß trotz einer zentralen Namensverwaltung ein dezentral angeordneter Abwickler angerufen wird.

Allein schon die Verwendung eines Codes für das Transaktionsprotokoll in einem Rechnernamen bietet so schon eine flexible Form der Verbindung von einem Terminal zu einem Abwickler.

Dabei wird ein gegen Manipulationen wie absichtliche, gezielte Verfälschung oder Ausspähung ein gesichertes Protokoll verwendet. Ein Beispiel hierfür eine solche Protokollfamilie ist in dem Entwurf "The SSL Protocol Version 3.0" von A.E.Freier, Ph. Karlton und P.C. Kocher vom März 1996 enthalten, der z. B. am 10.03.1997 unter der URL

ftp://ietf.cnri.reston.va.us/internet-drafts/draft-freier-ssl-version3-01.txt

bei der "Internet Engineering Task Force" (IEFT) abgerufen werden konnte. Dieses Protokoll erlaubt die Verwendung einer Vielzahl von kryptographischen Protokollen und Verfahren, um die gegenseitige Authentizität zu sichern und die übertragenen Daten gegen Manipulation und Ausspähung zu sichern.

Vorzugsweise wird dabei in dem Terminal **11**a' ein Sicherheitsmodul **19**a eingesetzt, in dem ein geheimer Schlüssel für den Aufbau der SSL-Verbindung gespeichert ist, der für dieses Terminal einzigartig und kennzeichnend ist. In bekannter Art ist im Falle eines symmetrischen Verfahrens dieser geheime Schlüssel in einem Sicherheitsmodul jedes Abwicklers, mit dem das Terminal Verbindung aufnehmen können soll, gespeichert. Bevorzugt werden jedoch asymmetrische Verfahren eingesetzt, bei denen nur im Sicherheitsmodul des Terminals ein privater Schlüssel gespeichert ist und der daraus abgeleitete Schlüssel als sogenannter öffentliche Schlüssel den Abwickeln zur Verfügung steht und lediglich für ihre Authentizität durch eine der bekannten Maßnahmen gesorgt werden muß. Der Sicherheitsmodul in dem Terminal wird also primär für die Sicherung der Verbindungen zu den Abwicklern benötigt, während die Sicherheitsmodule in den Abwicklern auch für die Sicherung der Chipkarten-Transaktionen und dem damit verbundenen herkömmlichen Key-Management dienen.

In einer Weiterbildung der Erfindung wird der Sicherheitsmodul des Terminals als Pufferspeicher für Schlüssel benutzt, die zusammen mit Programm-Moduln von einem Abwickler bezogen werden. Diese Programm-Moduln können dann unter Verwendung der im Sicherheitsmodul abgelegten Schlüssel eine Transaktion mit der Chipkarte lokal abwickeln. Handelt es sich um eine Geldkarte, so werden die Beträge auch, wie bei einer Geldkarte üblich, im Sicherheitsmodul abgelegt und erst am Tagesende kryptographisch gesichert übermittelt. Die Übermittlung erfolgt dabei bevorzugt an den Abwickler, der dem Terminal das Programm-Modul und den oder die zugehörigen Schlüssel über die gesicherte Netzwerkverbindung übertragen hat. Zur Leistungssteigerung können mehrere funktionsgleiche Abwickler vorhanden sein, die dann in diesem Sinn als dieselben Abwickler gelten sollen.

Einige Kartentypen können zwar die gesamte Transaktion lokal abwickeln, jedoch muß nach Transaktionsende ein Transaktionssatz über ein Netzwerk an eine Zentrale übermittelt werden. Auch in diesem Fall kann von dem Abwickler ein Programm-Modul übermittelt und in dem Terminal ausgeführt werden, welches dann den Transaktionssatz an seinen Abwickler schickt. Es kann durchaus sinnvoll sein, für jede Transaktion den Programm-Modul samt Schlüssel über die gesicherte Verbindung des Netzwerkes zu übertragen, anstatt die Transaktionsschritte einzeln zu übertragen. Insbesondere in einem Datagramm-orientierten Netzwerk wie dem Internet, bei dem gelegentliche Verzögerungen nicht auszuschließen sind, fällt dann eine Wartezeit allenfalls am Beginn oder Ende einer Transaktion an, aber nicht zwischen den einzelnen Transaktionsschritten.

Dabei werden die Programm-Moduln auf herkömmlichem Massenspeicher abgelegt, aber zur Sicherheit gegen Verfälschung signiert und gegebenenfalls auch verschlüsselt, wobei der passende Schlüssel zur Prüfung der Signatur auch in dem Sicherheitsmodul gespeichert ist. Die Auswahl der Programm-Moduln geschieht über die Kartenart bzw. einen daraus abgeleiteten Code. Terminal und Sicherheitsmodul können also als Pufferspeicher ("cache") angesehen werden. Indem insbesondere das Sicherheitsmodul zumindest teilweise als Pufferspeicher dient, ist eine praktisch beliebig große Anzahl von Chipkarten mit dem Terminal verwendbar und diese Anzahl ohne Wartungsarbeiten an dem Terminal, wie es das Hinzufügen eines weiteren Sicherheitsmoduls bedeuten würde, dynamisch erweiterbar.

Das Protokoll "HTTP" bzw. seine gesicherte Variante "HTTPS" erlaubt dabei eine besonders einfache Möglichkeit der Pufferung. In dem HTTP/1.0 beschreibenden Dokument RFC 1945 von Bernes-Lee u. a., Ausgabe Mai 1996, ist in Abschnitt 10.9 der Zusatz "if-modified-since" vorgesehen. Ein auf diese Art angefordertes Dokument wird nur dann übertragen, wenn es in neuerer Version vorliegt und kann auch zur Zwischenstationen gepuffert werden. Es ist also möglich, ein Programm-Modul samt benötigtem Schlüssel zu verpacken, verschlüsseln und zu signieren und mit einem durch einen URL bezeichneten Netzwerknamen zu versehen. Mit Einführen der Chipkarte bestimmt das Betriebsprogramm über den Code der Kartenart eine URL, fügt das Datum der vorhandenen, gepufferten Version hinzu und sendet eine Anforderung an den Abwickler. Ist die gepuf-

ferte Version aktuell, wird nur der Antwortcode "304" übertragen, und die gepufferte Version benutzt. Andernfalls wird die übertragene Version entpackt, abgelegt und ausgeführt.

In einer weiteren Variante können auch vor der Installation bereits Programm-Module und Schlüssel in dem Terminal derart abgelegt werden, als wenn sie über eine Netzverbindung übertragen und gepuffert worden seien. Dies ist für vorbekannt häufig oder überwiegend benutzte Anwendungen eine Möglichkeit, die Netzlast zu reduzieren. Auch kann ein Indikator in der Pufferspeicherverwaltung diese Einträge derart kennzeichnen, daß eine Verdrängung im Pufferspeicher vermieden werden oder ganz unterbleiben soll. Die jeweilige Anfrage bei dem durch die Chipkarte bestimmten Abwickler, ob dort eine neue Version vorliegt, ist davon nicht betroffen und ersetzt gegebenenfalls die vorgespeicherte Version.

Bevorzugt wird, wie beschrieben, der Programmodul zusammen mit einem oder mehreren Schlüsseln vom Abwickler in das Terminal übertragen. Es ist jedoch auch möglich, Programmoduln und Schlüssel getrennt zu verwalten und handzuhaben, wenn beispielsweise die dadurch erhöhte Netzbelastung der erhöhten Flexibilität entgegenkommt.

Durch die gegenüber den Beschränkungen der Chipkarte gesteigerten Rechenleistungen in einem Terminal, die in den bislang ausgegebenen und weiterzuverwendenden Chipkarten nicht gegeben ist, können nunmehr auch Public-Key-Verfahren für die Sicherung der Datenkommunikation, insbesondere die Authentisierung und Erzeugung von Sitzungsschlüsseln, eingesetzt werden. Weitere Angaben hierzu kann auch dem SSL-Dokument und den dort aufgeführten Literaturverweisen entnommen werden. Für die Zertifizierung öffentlicher Schlüssel können beispielsweise Zertifikate nach der Norm X509.3 dienen.

Das Sicherheitsmodul kann als Chipkarte oder als aus den GSM-Mobiltelefonen bekanntes SIM-Modul ausgeführt sein. Auch sind Sonderanfertigungen beispielsweise auf Basis des Chips SL 44CR80S der Firma Siemens möglich.

Nachdem die gesicherte Verbindung zwischen Terminal und Abwickler aufgebaut ist, vermittelt das Betriebsprogramm die Kommunikation zwischen Abwickler und Chipkarte. In den meisten Fällen werden dabei Datenblöcke von dem Betriebsprogramm in das Protokoll der Netzwerkverbindung umgesetzt und transparent vermittelt. In vielen Fällen wird jedoch eine Kommunikation mit einem Benutzer, sprich dem Besitzer der Chipkarte, benötigt, damit dieser den Wert der Transaktion angezeigt bekommt und die Transaktion anschließend bestätigen kann. Hierzu sind an dem Terminal Ein- und Ausgabeeinrichtungen wie Tastatur und Anzeige vorgesehen. Diese werden dem Abwickler über die gesicherte Verbindung zur Verfügung gestellt, denn nur der Abwickler besitzt den authentischen Wert für die Transaktion. Alternativ kann das Betriebsprogramm diese Daten aus der Kommunikation zwischen Chipkarte und Abwickler ermitteln und von sich aus anzeigen und die Bestätigung an den Abwickler übermitteln.

Als Terminal kann auch ein Personal Computer dienen, der mit einer Leseeinrichtung für Chipkarten ausgerüstet ist. Das Betriebsprogramm des Terminals wird auf dem Prozessor des PC ausgeführt und hat damit zusätzlich Zugriff auf den Bildschirm und die Tastatur. Damit kann insbesondere bei interaktivem Dialog, beispielsweise über einen Zugang zum Internet und dem WorldWideWeb, ein Bezahlvorgang ausgelöst werden. Besonders vorteilhaft ist dabei, daß die Erfindung zur Kommunikation zwischen Chipkarte und Abwickler dasselbe Datennetz, nämlich das Internet, verwenden kann, das bereits für den interaktiven Dialog benutzt wird. Bevorzugt enthält die Leseeinrichtung für die zur Bezahlung benutzte Chipkarte einen eigenen Prozessor und ein Sicherheitsmodul, vorzugsweise in Form einer weiteren, eingebauten Chipkarte. Der Prozessor auf der Leseeinrichtung übernimmt die Kommunikation zwischen Chipkarte und Abwickler und wendet sich an den Prozessor des Personal Computers für Dialoge mit dem Benutzer.

Sofern das damit erreichbare Sicherheitsniveau für den Benutzer eines Personal Computers akzeptabel ist, kann auch auf einen besonderen Sicherheitsmodul und einen Prozessor auf der Leseeinrichtung verzichtet werden. Dies ist der Fall, wenn der PC nicht allgemein, sondern nur wenigen bekannten Personen zugänglich ist und eine Verfälschung des Betriebsprogramms nicht zu befürchten ist, wie es sich in der Wohnung eines Privatanwenders darstellt. Für den Manipulationsschutz der Kommunikation mit dem Abwickler kann auch gänzlich auf einen permanenten geheimen Schlüssel verzichtet werden, indem beispielsweise für die Kommunikation Sitzungsschlüssel nach dem Verfahren von Diffie und Hellmann gebildet werden. Je nach Anwendungsfall ist denkbar, daß die Authentizität des Terminals für den Abwickler nicht unabdingbar ist, da die eigentlichen Transaktionen mit der Chipkarte abgewickelt werden.

Anstelle von speziellen Terminals beispielsweise in Verbindung mit Kassen oder Personal Computern kann ein Terminal nach der Erfindung auch in einen Waren- oder Dienstleistungsautomaten, Informationsterminals eingeschlossen, eingebaut sein. Ein- und Ausgabeeinheiten sind dann beispielsweise die Wahltaster für eine Ware und die Ausgabemechanik für die gewählte Ware.

Es ist auch denkbar, daß Chipkarten ausgegeben werden, die als weitere Anwendung die Erzeugung von Sitzungsschlüsseln für eine gesicherte Internet-Verbindung nach beispielsweise dem SSL-Protokoll enthalten. Damit ist dann auf Personal Computern auf der Leseeinrichtung für Chipkarten weder ein eigener Prozessor noch ein Sicherheitsmodul notwendig.

In **Fig.** 1 nicht dargestellt, kann jeder Host **16a**, **16c** auch mit dem offenen Datennetz **12** verbunden sein und die Abwicklerfunktion direkt unterstützen, sofern Sicherheitserwägungen nicht dagegen sprechen.

Ein besonderer Vorteil der Erfindung liegt darin, daß lediglich die Abwickler angepaßt werden müssen bzw. zusätzliche Abwickler bereitgestellt werden müssen, die Netzwerke **15a**, **15c** für die Transaktionsabwicklung und die Host-Anwendungen **16a**, **16c** unverändert bestehen bleiben können und damit die bisherigen Anwendungen unverändert weiterbetrieben werden können.

Da ein Terminal auch zusätzlich zu einem Chipkartenleser mit einem Magnetkartenleser beziehungsweise einem Kombinationsleser ausgestattet werden kann, ist in einer Fortbildung das Betriebsprogramm dahin erweitert, daß es die Daten der Magnetspur und eventuell vorhandene Sicherheitsmerkmale an den Abwickler übertragen kann. Damit können die bisherigen, auf Magnetkarte basierenden Verfahren weiter benutzt werden. Dies gilt in gleicher Weise auch für Chipkarten ohne Prozessor, die einen Speicher zu lesen und zu beschreiben erlauben. In dem Maße, wie diese Karten aus dem Verkehr geraten, kann die Anzahl der Abwickler im Netz reduziert werden.

Ein Sicherheitsvorteil ergibt sich dadurch, daß die für die Transaktionsabwicklung notwendigen geheimen Schlüssel nicht mehr in dem Terminal gespeichert sein müssen. Dies hat bislang dazu geführt, daß Terminals bei öffentlicher Aufstellung besonders geschützt wurden, um jeden Angreifer auf den Sicherheitsmodul von vornherein zu entmutigen. Ein erfolgreicher Angriff auf einen Sicherheitsmodul, der lediglich die Kommunikation zwischen Terminal und Abwickler betrifft, hat weniger gravierende Auswirkungen als einer auf einen herkömmlichen Sicherheitsmodul. Auch

können die Abwickler als Prozesse auf Hochleistungsrechnern ablaufen, so daß eine besonders schnelle Reaktion möglich ist und eine Vielzahl von Abwicklern einen gemeinsamen schnellen Sicherheitsmodul benutzen können.

Patentansprüche

1. Verfahren zur Abwicklung von Transaktionen, die durch eine Chipkarte gesichert werden, die mit einem Terminal verbindbar ist, welches an ein Datennetzwerk angeschlossen ist, mit den Merkmalen:
   - Das Terminal enthält ein Betriebsprogramm, welches nach dem Verbinden der Chipkarte mit dem Terminal einen Code für ein Transaktionsverfahren, nach dem die Transaktion durchzuführen ist, bestimmt,
   - aus dem Code des Transaktionsverfahrens wird die Netzwerkadresse eines Abwicklers bestimmt,
   - woraufhin das Betriebsprogramm eine durch kryptographische Verfahren gesicherte Verbindung zu dem Abwickler aufbaut,
   - danach die Transaktion durch Vermittlung zwischen Chipkarte und Abwickler abwickelt.
2. Verfahren nach Anspruch 1, wobei insbesondere zur Bestätigung der Transaktion an das Terminal angeschlossene Ein- und Ausgabeeinheiten durch die Datenverbindung zwischen Terminal und Abwickler für den Abwickler benutzbar sind.
3. Verfahren nach Anspruch 1 oder 2, wobei der Abwickler sowohl zur Sicherung der Verbindung mit dem Terminal wie auch zur Sicherung der Transaktionen mit der Chipkarte gesicherte Schlüssel mindestens eines direkt verbundenen Sicherheitsmoduls verwendet.
4. Verfahren nach Anspruch 3, wobei das Terminal zur Sicherung der Verbindung mit dem Abwickler gesicherte Schlüssel eines direkt verbundenen Sicherheitsmoduls verwendet.
5. Verfahren nach Anspruch 4, wobei zur Sicherung der Verbindung zwischen Terminal und Abwickler eine Anwendung der Chipkarte und ein gesichert in der Chipkarte gespeicherter Schlüssel verwendet wird, mittels derer ein Sitzungsschlüssel für die weitere Abwicklung der Transaktion bestimmt oder ein öffentlicher Schlüssel verifiziert wird.
6. Verfahren nach einem der Ansprüche 1 bis 5, wobei zur Verbindung von Terminal und Abwickler ein TCP/IP Protokoll verwendet wird.
7. Verfahren nach Anspruch 6, wobei zur Sicherung der TCP/IP Verbindung das Protokoll SSL verwendet wird.
8. Verfahren nach einem der Ansprüche 1 bis 7, wobei die Bestimmung der Netzwerkadresse eines für das Transaktionsverfahren geeigneten Abwicklers durch eine Anfrage bei einem dem Terminal zugeordneten Abwickler ermittelt wird.
9. Verfahren nach Anspruch 1 bis 7, wobei die Bestimmung der Netzwerkadresse eines für das Transaktionsverfahren geeigneten Abwicklers dadurch ermittelt wird, daß der Code das Transaktionsverfahren als Teil einer symbolischen Netzwerkadresse verwendet wird, welche durch dem Netzwerk angehörende Server für die Bestimmung von Netzwerkadressen aufgelöst wird.
10. Verfahren nach einem der Ansprüche 2 bis 9, wobei das Betriebsprogramm des Terminals den Benutzer zur Eingabe einer geheimen Zeichenkette auffordert, diesen gegen ein Referenzwert, insbesondere unter Anwendung von kryptographischen Verfahren, überprüft und lediglich das Ergebnis der Überprüfung über die gesicherte Verbindung an den Abwickler überträgt.
11. Verfahren nach einem der Ansprüche 1 bis 9, wobei mittels der Verbindung ein Programmodul vom Abwickler zu dem Terminal übertragen und dort anstelle mindestens eines Teils des Programmcodes des Abwicklers ausgeführt wird.
12. Verfahren nach einem der Ansprüche 4 bis 9, wobei mittels der Verbindung ein Schlüssel vom Abwickler in das Sicherheitsmodul übertragen wird und zur gesicherten Abwicklung mindestens eines Teils einer Transaktion mit der Chipkarte dient.
13. Verfahren nach Anspruch 11 oder 12, wobei die von dem Abwickler übertragenen Programmoduln oder Schlüssel in der Art eines Pufferspeichers im Terminal abgelegt werden und anstelle einer erneuten Übertragung verwendet werden.
14. Verfahren nach Anspruch 13, wobei vor einer Benutzung eines gepufferten Programmoduls oder Schlüssels durch eine Anfrage an den Abwickler die Aktualität überprüft und gegebenenfalls eine aktuelle Version übertragen und zukünftig verwendet wird.
15. Verfahren nach Anspruch 14, wobei zur Anforderung mit Aktualitätsprüfung das Protokoll HTTP oder HTTPS verwendet wird.
16. Anordnung zur Abwicklung von Transaktionen, die durch eine Chipkarte gesichert werden, die mit einem Terminal verbindbar ist, welches an ein Datennetzwerk angeschlossen ist, mit den Merkmalen:
   - Das Terminal enthält eine Einrichtung, die mittels der Verbindung der Chipkarte zum Terminal einen Code für das zu benutzende Transaktionsverfahren bestimmt,
   - aus dem Code wird durch ein Mittel zur Adressabbildung ein über das Datennetzwerk erreichbaren Abwickler adressiert,
   - das Terminal enthält eine Verbindungseinrichtung, die eine Verbindung zu dem Abwickler herzustellen vermag,
   - das Terminal und der Abwickler enthalten Vorrichtungen, mit denen die Verbindung zwischen Terminal und Abwickler gegen Manipulationen sicherbar ist,
   - der Abwickler enthält Einrichtungen, die Transaktionen mit der Chipkarte unter Vermittlung des Terminals gesichert abzuwickeln gestatten.
17. Anordnung nach Anspruch 16, wobei das Terminal Ein-Ausgabevorrichtungen enthält, die von dem Abwickler über das Netzwerk während er Abwicklung der Transaktion benutzbar sind.
18. Anordnung nach Anspruch 16 oder 17, wobei der Abwickler mindestens eine Einrichtung für die sichere Speicherung von kryptographischen Schlüsseln sowohl für die Sicherung der Verbindung zum Betriebsprogramm des Terminals als auch für die Sicherung der Transaktion mit der Chipkarte enthält.
19. Anordnung nach Anspruch 18, wobei das Terminal eine Einrichtung für die sichere Speicherung von Schlüsseln für die Sicherung der Verbindung mit dem Abwickler umfaßt.
20. Anordnung nach Anspruch 19, wobei die Chipkarte eine Einrichtung umfaßt, mit der ein Sitzungsschlüssel für die Sicherung der Verbindung zwischen Terminal und Abwickler in dem Terminal erzeugbar ist.

Hierzu 2 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 197 10 249 A1
Int. Cl.[6]: G 07 F 19/00
Offenlegungstag: 17. September 1998

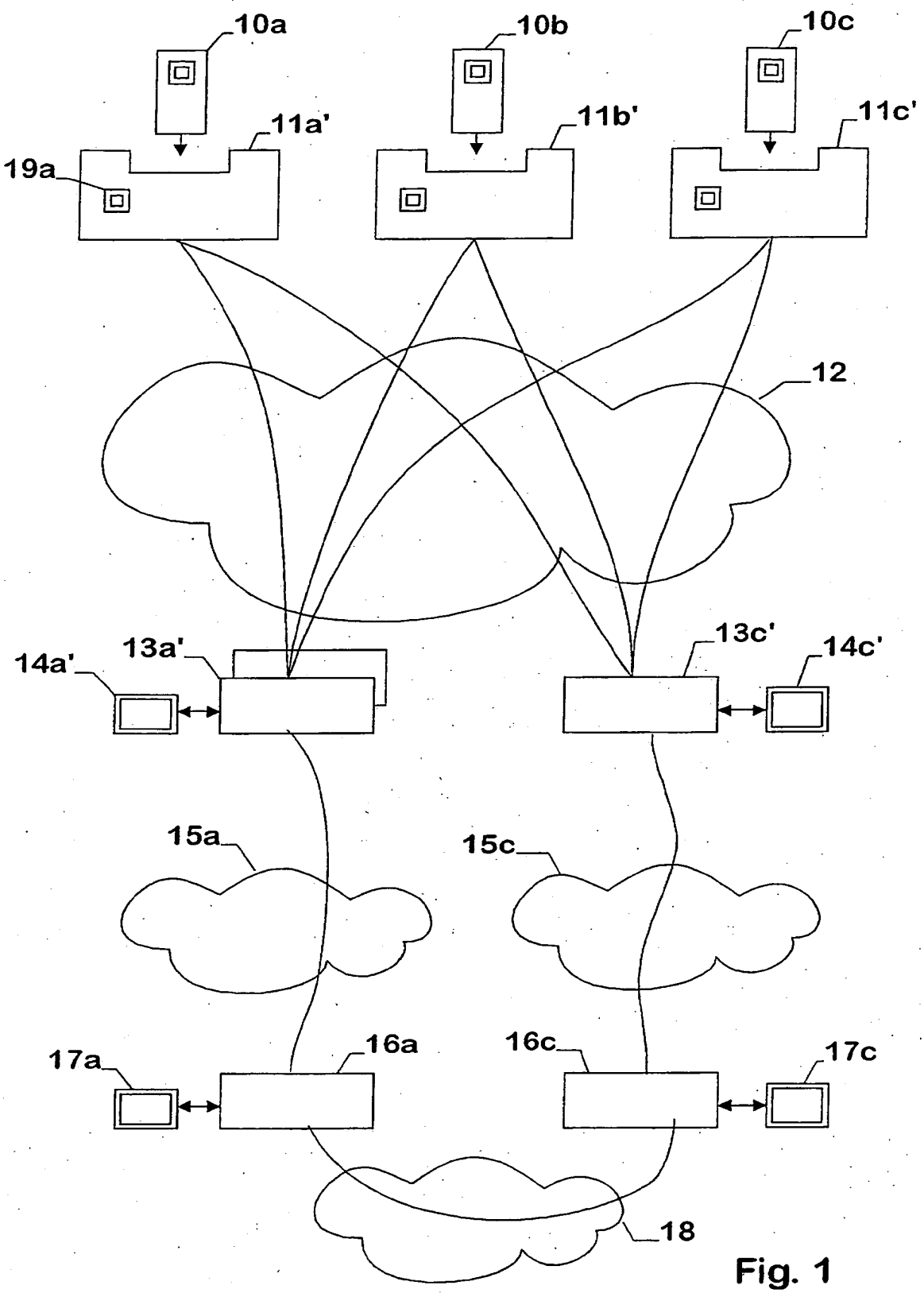


Fig. 1

Nummer: DE 197 10 249 A1
Int. Cl.[6]: G 07 F 19/00
Offenlegungstag: 17. September 1998

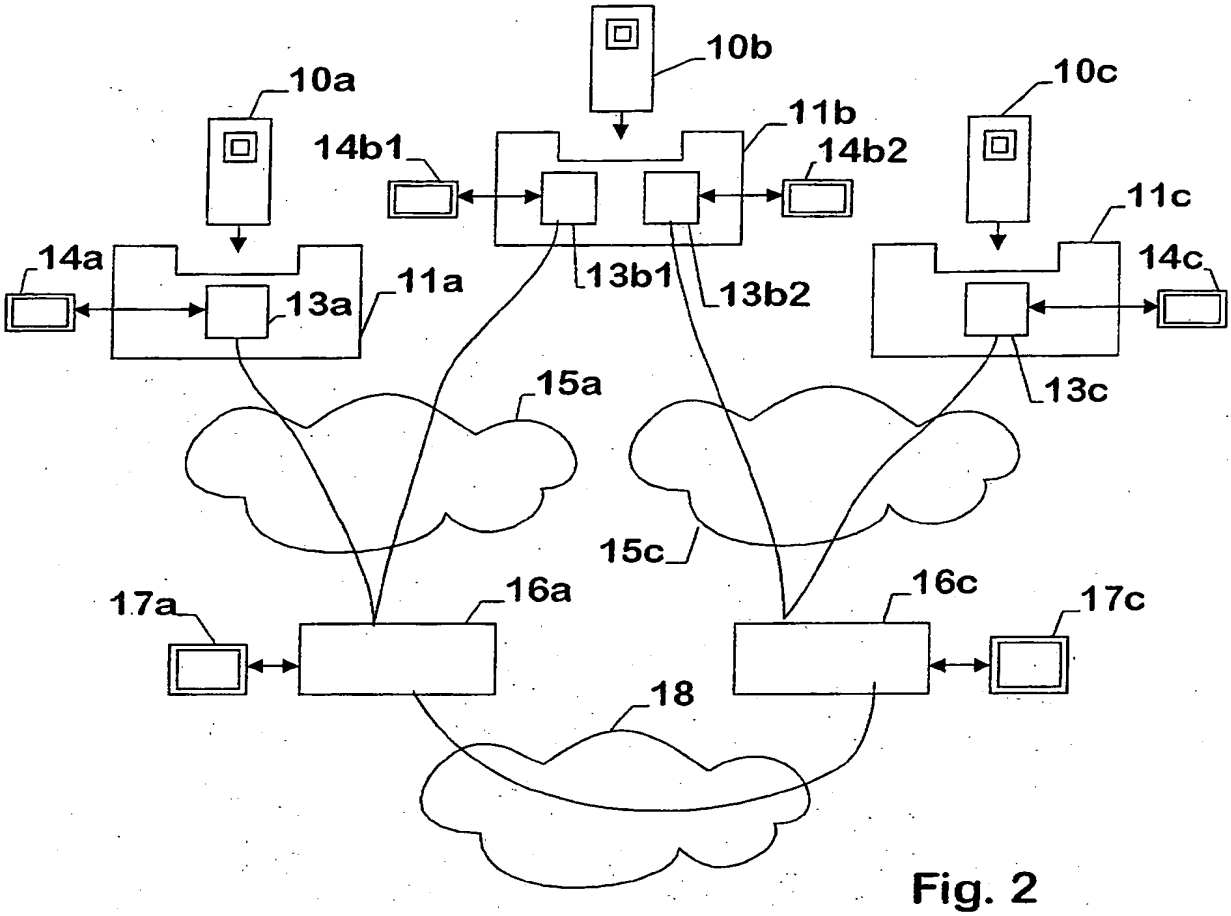


Fig. 2